GCCSI

Ihr Dienstleister in:

Gürbüz Computer Consulting & Service International 1984-2007 l Önder Gürbüz l Aar Strasse 70 l 65232 Taunusstein
info@gccsi.com l +49 (6128) 757583 l +49 (6128) 757584 l +49 (171) 4213566

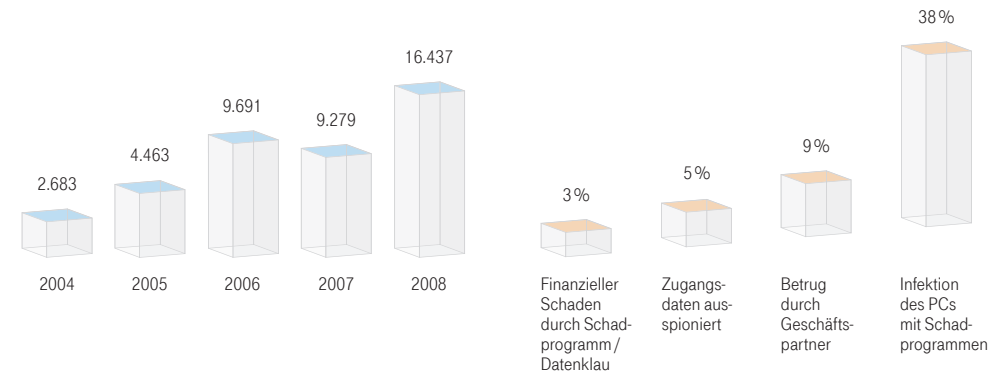
Datenschutz zu Hause – gewusst wie!

Erleben, was verbindet.

Datenschutz zu Hause – gewusst wie!

FSC Mix
Produktgruppe aus vorbildlich bewirtschafteten Wäldern und anderen kontrollierten Herkünften
www.fsc.org Zert.-Nr. SGS-COC-003628
© 1996 Forest Stewardship Council

Internetkriminalität steigt weiter an – jeder Zweite betroffen



Quelle: BITKOM/Forsa (2009), Basis: Internetnutzer ab 14 Jahren

Nach einer Schätzung des BITKOM für das Jahr 2009 entstand allein für die Nutzer von Online-Banking eine Schadenssumme von 11 Millionen Euro. Und das ist nur einer von vielen Fakten im Zusammenhang mit der zunehmenden Internetkriminalität.

Vorwort.

Wir wollen mit diesem Ratgeber darauf aufmerksam machen, dass Datenschutz mehr ist, als nur ein funktionierendes Antivirenprogramm auf dem Computer zu installieren.
Wir leben im Zeitalter der Digitalisierung – wir erledigen unsere privaten Bankgeschäfte online, kaufen über das Internet ein und pflegen immer häufiger unsere sozialen Kontakte im Netz. Mit dem Verhalten der Nutzer hat sich auch die Kriminalität verändert. Das Ausspionieren von Zugangsdaten oder das Knacken von privaten WLAN-Verbindungen sind die modernen Varianten des Handtaschendiebstahls und des Einbruchs. Jeder weiß, wie mit einigen Handgriffen Haus und Handtaschen gesichert werden. Wir sollten für die Nutzung des Internets die gleiche Routine entwickeln.

Indem Sie die folgenden Tipps beachten, können Sie sich vor Internetkriminalität schützen und Missbrauch vorbeugen. Wenn Sie Fragen zum Thema Datenschutz allgemein oder bei der Deutschen Telekom haben, können Sie sich im Internet unter **www.telekom.com/datenschutz** informieren oder eine E-Mail an **datenschutz@telekom.de** schicken.

Ihr Claus-Dieter Ulmer

Konzerndatenschutzbeauftragter
Deutsche Telekom

PC-Sicherheit und Basisschutz.

Damit Ihre privaten Daten auf dem PC auch privat und sicher bleiben, beachten Sie die folgenden Tipps.

Machen Sie sich immer bewusst, wie sensibel die Daten sind.

Bei vertraulichen Informationen sollten Sie keinen öffentlichen PC verwenden, da Sie nicht wissen, ob dieser ausreichend gegen →**Viren,** →**Würmer,** →**Trojaner** und äußere Angriffe geschützt ist.

Schützen Sie Ihren PC vor Einblicken. Achten Sie darauf, wer Einblick auf Ihren Bildschirm hat, wenn Sie sensible Daten wie Benutzernamen und Kennwörter eingeben.

Halten Sie Ihr System immer auf dem aktuellen Stand.

Softwareanbieter entwickeln ihre Produkte ständig weiter und schließen damit aufkommende Sicherheitslücken. Halten Sie daher Ihre Software und besonders die Virenschutzsoftware auf dem aktuellsten Stand, um sich vor Angriffen zu schützen. Die Telekom bietet ein Sicherheitspaket an, das vor diesen Angriffen schützt und monatlich gebucht werden kann.
www.t-online.de/sicherheitspaket

Gewährleisten Sie hohe Sicherheitseinstellungen.

Um Ihre Daten zu schützen, installieren Sie ein Virenschutzprogramm und ein →**Anti-Spyware**-Programm. Wichtig ist auch, dass Sie Ihre persönliche →**Firewall** einrichten. Durch die Konfiguration schützen Sie sich vor Angriffen aus dem Internet. Nutzen Sie auch den Viren-Scanner Ihres E-Mail-Anbieters, um einen möglichst hohen Sicherheitsstandard zu erhalten.

Prüfen Sie Downloads und E-Mail-Anhänge.

Viren werden gerne über Dateianhänge verbreitet. Öffnen Sie daher nur vertrauenswürdige Anhänge von Personen, die Sie tatsächlich kennen. Bei Software-Downloads verhält es sich ähnlich: Wenn Ihnen der Anbieter oder die Seite nicht Vertrauen erweckend erscheint, sollten Sie den Download nicht ausführen.

Sichern Sie Ihren PC mit Kennwort.

Damit Sie Ihren PC und damit Ihre Daten vor dem Zugriff Dritter schützen, sollten Sie ihn immer durch ein Passwort sperren. Achten Sie darauf, dass das Passwort ein sehr sicheres ist.

Nach Eingabe des korrekten Passworts wird der Bildschirm wieder freigegeben und Sie können Ihre Arbeit fortsetzen. Empfohlen wird, dass die Bildschirm- und Tastatursperre fünf Minuten nach der letzten Benutzereingabe mit dem Bildschirmschoner einsetzt. Im privaten Bereich ist die Aktivierungszeit natürlich frei wählbar. Nach Bedarf kann man die Sperre auch sofort aktivieren. Das geht bei einem Windows-Betriebssystem, indem man die Tastenkombination Strg + Alt + Entf drückt und dann die Option „Arbeitsstation sperren“ auswählt.

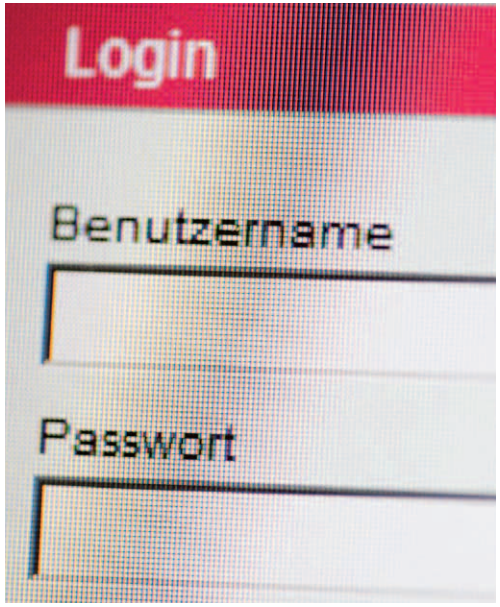
Schalten Sie Funkschnittstellen aus.

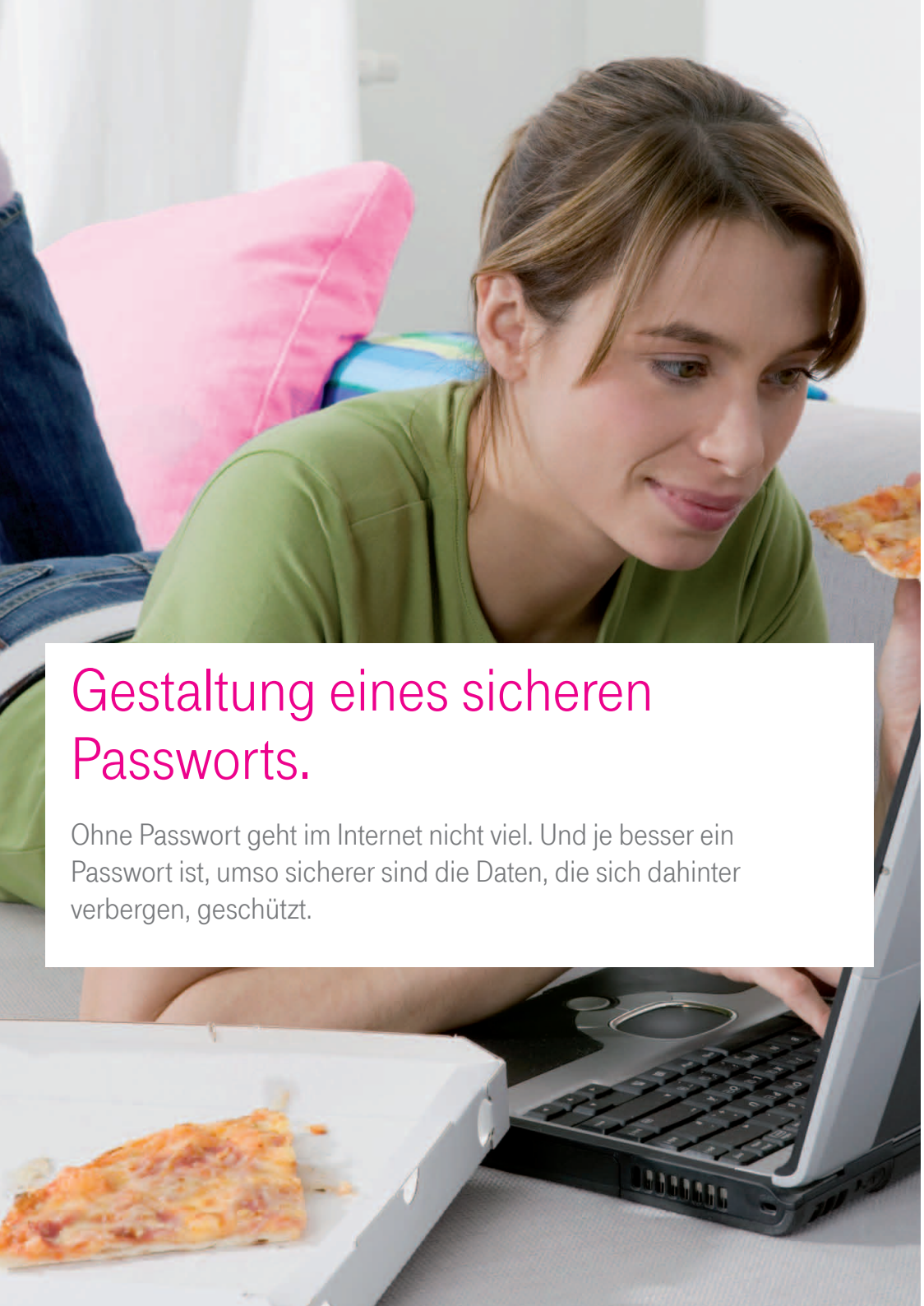
Um Ihren privaten PC vor Angriffen von außen zu schützen, schalten Sie alle nicht aktuell benötigten Funkschnittstellen ab – wenn Sie aus dem Raum gehen, machen Sie ja auch das Licht aus! Also warum nicht den →**WLAN**-Sender am Router ausschalten, wenn Sie nicht im Internet sind? Die meisten Modelle haben heute einen Knopf auf der Rückseite. Das Gleiche gilt auch für Ihr Handy beispielsweise bei der →**Bluetooth**-Schnittstelle, um es zum einen vor Viren, Würmern und Trojanern zu schützen und um zum anderen Unbefugten nicht den Zugang zu Ihren persönlichen Daten wie dem Adressbuch, dem Kalender oder Ihren Bildern zu ermöglichen.

Konfigurieren Sie Ihre drahtlosen Zugänge auf die von Ihnen genutzten Geräte. Damit erschweren Sie Dritten zusätzlich den Zugang (siehe „WLAN-Sicherheit“).

Datensicherung.

Damit Sie ganz sichergehen, sollten Sie besonders von wichtigen Daten regelmäßig eine Sicherheitskopie, zum Beispiel auf CD-ROM / DVD oder einer externen Festplatte, anfertigen.





Gestaltung eines sicheren Passworts.

Ohne Passwort geht im Internet nicht viel. Und je besser ein Passwort ist, umso sicherer sind die Daten, die sich dahinter verbergen, geschützt.

Online-Banking, E-Mails lesen oder einen Beitrag im Anglerforum schreiben – wer sich im → Web 2.0 bewegt, kommt früher oder später immer an einen Punkt, an dem Anmeldename und Passwort gefragt sind. Der Anmeldename bereitet dabei meist keine Probleme. Doch spätestens beim fünften Passwort wird es schwierig, noch den Überblick zu behalten. Dazu kommt, dass ein sicheres Passwort leider das Gegenteil von einprägsam ist. Wie erstelle ich also ein sicheres Passwort, das sich merken lässt? Hier erfahren Sie, wie Sie Hacker zur Verzweiflung bringen und Ihre Daten schützen.

Wie erstelle ich ein sicheres Passwort?

Die goldene Regel für ein sicheres Passwort lautet: Es sollte von Außenstehenden nicht als sinnvolles Wort erkannt werden. Um ein solches Passwort zu erhalten, gibt es einen einfachen Trick: Denken Sie sich einen Satz aus, den Sie sich gut merken können. Von diesem Satz verwenden Sie nur die Anfangsbuchstaben und ersetzen einzelne Buchstaben durch Zahlen und Sonderzeichen.
Ein Beispiel für einen solchen Satz wäre: „Wir zwei essen gerne Pizza mit Salami."
Die Anfangsbuchstaben ergeben die Kombination „WzegPmS". Nun kommen die Zahlen und Sonderzeichen ins Spiel. Hier können Sie Ihrer Fantasie freien Lauf lassen. Bei unserem Beispielsatz ersetzen wir das „z" durch eine „2" und fügen am Ende noch ein „!" an. Unser sicheres Passwort lautet dann „W2egPmS!". Dieses Passwort besteht aus 8 Zeichen. Dies ist die Untergrenze, die Experten für ein sicheres Passwort empfehlen. Grundsätzlich gilt: Je länger und komplexer ein Passwort ist, desto besser.

Der Grund: Hacker probieren mit Programmen systematisch alle Möglichkeiten aus, wie ein Passwort aufgebaut sein kann. Mit jedem zusätzlichen Zeichen steigt also die Zahl der möglichen Passwörter und damit auch die der nötigen Durchläufe, die ein solches Computerprogramm zum Knacken Ihres Passworts benötigt.

Erstellen Sie für jeden Zugang ein Passwort.

Eine weitere wichtige Vorsichtsmaßnahme: Verwenden Sie nach Möglichkeit für unterschiedliche Zugänge unterschiedliche Passwörter. Denn ab und an gelingt es Datendieben, ganze Kundendateien inklusive aller Zugangsdaten auszuspionieren. Ein Passwort, das den Dieben so in die Hände fällt, ist nicht mehr sicher. Denn die Hacker werden auch

Generell gilt: Überlegen Sie sich gut, was es für Folgen hätte, wenn Ihr Passwort in die falschen Hände fallen würde – und treffen Sie danach Ihre Entscheidung, wie sicher Sie Ihr Passwort gestalten.

dieses Passwort ausprobieren, wenn sie sich einen Zugang erschleichen wollen. Ein sicheres Passwort ist also immer eines, das Sie nur für einen Zugang verwenden. Das sollte auf jeden Fall für Ihren Zugang zum Online-Banking gelten.

Bewahren Sie Passwörter sicher auf.

Zusätzlich sollten Sie Ihre Passwörter nur an sicheren Plätzen aufbewahren, zu denen nur Sie Zugang haben. Der beste Platz dafür ist natürlich Ihr Kopf. Der schlechteste Platz ist wohl Ihr Browser. Sie sollten daher vor allem bei wichtigen Passwörtern auf die „Auto-vervollständigen-Funktion“ verzichten und sie nie auf der Festplatte speichern oder auf einem Zettel in der Nähe des PCs notieren.

Ändern Sie Passwörter regelmäßig.

In regelmäßigen Abständen sollten Sie Ihr Passwort ändern, um den Schutz vor Datendiebstahl zu erhöhen. Wir empfehlen Ihnen, das mindestens alle drei Monate zu tun.

Wann benötige ich ein sicheres Passwort?

Das Problem bei sicheren Passwörtern ist: Sie sind unheimlich schwer zu merken. Egal ob der Name der Ehefrau oder der Geburtstag der Oma – jede Gedächtnisstütze macht ein Passwort unsicherer. Doch möglicherweise benötigen Sie nicht immer ein Passwort, das absolut sicher ist. Etwa beim oben genannten Anglerforum müssen Sie vermutlich nicht so vorsichtig sein wie beim Online-Banking.

Überlegen Sie daher gut, bevor Sie ein Passwort wählen:

- Schützt es persönliche oder geschäftliche Informationen (z. B. E-Mails, Kontakte etc.)?
- Können mit dem Zugang finanzielle Transaktionen getätigt werden (wie beispielsweise beim Online-Banking oder bei Internet-Auktionshäusern)?
- Haben Sie bei dem entsprechenden Zugang wichtige Daten, etwa Ihre Kreditkartennummer oder Bankverbindung, hinterlegt?

Wenn Sie eine dieser Fragen mit Ja beantworten, dann sollten Sie unbedingt ein möglichst sicheres Passwort wählen. Falls nicht, genügt möglicherweise auch ein weniger sicheres Passwort. Natürlich sollten Sie auch hier darauf achten, es eventuellen Hackern nicht zu leicht zu machen.

WLAN-Sicherheit.

Immer mehr Menschen benutzen zu Hause oder im öffentlichen Raum drahtlose Funknetzwerke (Wireless Local Area Networks, kurz WLAN), um ins Internet zu kommen.

Sie sind praktisch, da von jedem beliebigen Ort der Zugang ins Internet möglich ist. Sie bergen aber auch Sicherheitsrisiken. Generell kann man sagen, dass jede drahtlose Verbindung weniger Sicherheit bietet als eine Netzwerkverbindung per Kabel. Bei der drahtlosen Verbindung werden die Daten per Funk an den Empfänger übermittelt und können abgefangen werden.

Laut eines Urteils des Bundesgerichtshofs (BGH) vom 12. Mai 2010 (I ZR 121/08) ist jeder private WLAN-Betreiber dazu verpflichtet, sein Netz mit einem Passwort zu schützen. Verschafft sich ein Dritter unerlaubt Zugang zu Ihrem ungesicherten WLAN und führt illegale Handlungen durch, können Sie als Inhaber von einem dadurch Geschädigten zur Unterlassung und zur Erstattung der damit verbundenen Rechtsverfolgungskosten gezwungen werden.

Daher ist es wichtig, dass Sie Ihren WLAN-Router verschlüsseln, damit Ihre privaten E-Mails, Benutzernamen und Kennwörter nicht in die falschen Hände gelangen.

Übrigens: Die →**WLAN**-Router der Deutschen Telekom sind von Stiftung Warentest hinsichtlich ihres Sicherheitszustands in der ausgelieferten Version als beste Router im Test bewertet worden. Die wichtigen Informationen zur Konfiguration finden Sie in der Betriebsanleitung des Routers.

In Ihrem Haushalt können Sie sich vor Datendieben schützen, indem Sie folgende Punkte beachten.

Sichern Sie Ihren WLAN-Router.

Dies ist die wichtigste Vorsichtsmaßnahme, da der → **WLAN**-Router die Verbindung zwischen Ihrem Computer und Ihrem Internetanschluss herstellt. Bevor Sie Ihr WLAN in Betrieb nehmen, sollten Sie einige Grundeinstellungen ändern: Zunächst sollten Sie die → **SSID**, die den Netzwerknamen bezeichnet, manuell ändern und ihr einen persönlichen Namen geben. Wählen Sie dabei lieber einen Fantasienamen, der keine Rückschlüsse auf Sie persönlich oder Ihren Internetanbieter zulässt. Um die Sicherheit zu erhöhen, sollte die Ausstrahlung der SSID verhindert werden, damit der Name Ihres Routers im Netzwerk nicht gefunden werden kann. Da Sie den Namen Ihres Routers kennen, werden Sie ihn selbstverständlich finden.

Richten Sie eine Verschlüsselung ein.

Eine weitere Schutzmaßnahme ist die Verschlüsselung Ihres WLAN. Diese geschieht bei den meisten WLAN-Systemen über → **WPA2-PSK** – PSK (Pre-Shared Key), übersetzt: vorher vereinbarter Schlüssel. Dabei wird beim Verbindungsaufbau ein „Schlüssel" (Passwort) gebraucht, um ins Netz zu kommen. Wichtig ist, dass Sie hier einen sicheren Kennwortschutz wählen. Mehr Informationen zur Erstellung von Passwörtern finden Sie unter dem Punkt „Gestaltung eines sicheren Passworts".

Richten Sie einen Filter gegen Datendiebe ein.

Um die Sicherheit der eigenen Daten zu erhöhen, können Sie einen → **MAC-Adressen**-Filter einrichten. Die MAC-Adresse ist eine Nummer, mit der sich jede Netzwerkkarte und damit jeder internetfähige Computer identifizieren lässt. Wenn Sie nur die von Ihnen benötigten MAC-Adressen zulassen, haben fremde Computer keine Chance. Wie finde ich die MAC-Adresse? Beispiel Windows: Gehen Sie im Startmenü in den Bereich „Systemsteuerung". Dort klicken Sie auf das Symbol „System" und wählen im Bereich „Hardware" den Geräte-Manager. Dort finden Sie den Punkt „Netzwerkadapter". Normalerweise finden sich dort zwei Einträge – einer trägt im Namen meist den Zusatz „Wireless". Nach einem Doppelklick auf diesen Eintrag finden Sie verschiedene Menüs vor: Dort steht im Bereich „Erweitert" die MAC-Adresse.

Schalten Sie Ihr WLAN ab.

Wenn Sie Ihr WLAN nicht nutzen, sollten Sie es abschalten. Auf diese Art und Weise schützen Sie sich nicht nur vor Datendieben, sondern sparen auch Strom.

Besonders wenn Sie die öffentlich zugänglichen HotSpots nutzen, sollten Sie die hier folgenden Tipps berücksichtigen, um Ihre Daten bestmöglich zu schützen.

Sicherheitsinformation des BSI.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) empfiehlt zudem, sämtliche Einstellungen an einem WLAN-Router bei der Einrichtung Ihres WLAN über ein Kabel und nicht drahtlos durchzuführen.

Deaktivieren Sie Ihre Netzwerkfreigabe.

Wenn Sie → **HotSpots** nutzen, sollte die Datei- und Verzeichnisfreigabe auf Ihrem Laptop oder dem mobilen Endgerät deaktiviert sein. In der Regel können Sie diese Freigabe in den Netzwerkeinstellungen Ihres Betriebssystems deaktivieren. Sie sollten nie mit einem Benutzerkonto angemeldet sein, das Administratorenrechte besitzt.

Aktivieren Sie Ihre Firewall.

Bevor Sie sich in ein fremdes WLAN einwählen, aktivieren Sie Ihre → **Firewall**. Die Firewall überwacht den Datenverkehr von und zu Ihrem Rechner und hilft so dabei, Angriffe von Schadsoftware zu unterbinden.

Stellen Sie keine automatische Verbindung her.

Stellen Sie keine Verbindung mit dem HotSpot her, wenn Sie nicht wissen, wer für das Betreiben des Zugangs verantwortlich ist. Sie sollten auch keine automatische Verbindung mit Drahtlosnetzwerken zulassen, sondern immer manuell auswählen, mit welchem Netz Sie sich verbinden möchten.

Achtung bei falschen HotSpots.

Um an vertrauliche Daten zu gelangen, richten Kriminelle eigene drahtlose Netzwerke ein, die der Startseite des tatsächlichen HotSpot, beispielsweise von T-Mobile, sehr ähnlich sind. Bei der Verbindung mit dem falschen HotSpot werden Sie aufgefordert, Informationen, wie zum Beispiel Ihre Kreditkartennummer, anzugeben, angeblich um ein neues HotSpot-Konto zu eröffnen. Diese Manipulationstechnik ist angelehnt an die → **Phishing**- und → **Pharming**-Technik, die in dem Punkt „Sicheres Online-Banking und Schutz vor Phishing-Angriffen" erläutert wird.

Über die richtige Installation und Einrichtung eines sicheren WLAN-Zugangs können Sie sich auf **http://hilfe.telekom.de** informieren.

Sicheres Online-Banking und Schutz vor Phishing-Angriffen.

Immer mehr Menschen wickeln ihre Bankgeschäfte über das Internet ab. Diese Bankfiliale ist zu jeder Tages- und Nachtzeit erreichbar und kann bequem von zu Hause aus bedient werden.

So bequem das Online-Banking von zu Hause auch ist, es birgt Risiken, da mit sensiblen Daten gearbeitet wird. Daten wie → **PIN**- und → **TAN**-Nummern, die den Zugriff auf das Konto ermöglichen, fallen bei Unachtsamkeit immer wieder Betrügern in die Hände. Dies passiert sehr häufig durch Phishing-Angriffe, die auch nach Einschätzung des Bundeskriminalamts ein hohes Gefährdungs- und Schadenspotenzial besitzen. Phishing ist eine Wortzusammensetzung aus den Begriffen „Password" und „Fishing" und bezeichnet das Abgreifen von Passwörtern sowie PIN- und TAN-Nummern. Durch gefälschte E-Mails und Internetseiten, mit denen der Kunde aufgefordert wird, seine Kontodaten inklusive Passwörtern anzugeben, gelangen Kriminelle an die sensiblen Daten. Meist leitet ein Link die Benutzer auf die gefälschten Webseiten von Banken und anderen Unternehmen, die dem Original sehr ähnlich sehen.

Damit Sie sich vor diesen Angriffen schützen können, achten Sie auf die folgenden Punkte:

Achtung bei Phishing-E-Mails!

- In den meisten Fällen hat das Anschreiben der gefälschten E-Mail eine allgemeine, unpersönliche Anrede, zum Beispiel „Lieber Kunde der XY Bank".
- Bei einer Phishing-E-Mail wird zu einer zügigen und notwendigen Handlung aufgefordert, wobei auch Drohungen verwendet werden („Wenn Sie nicht sofort Ihre Daten aktualisieren, gehen diese verloren …").
- Achten Sie immer auf die komplette Absenderadresse der E-Mail. Wenn die Adresse nicht eindeutig Ihrer Bank zuzuordnen ist, fragen Sie lieber noch einmal direkt nach und sichern sich ab.
- Ihre Bank wird Sie nie auffordern, vertrauliche Daten wie etwa PIN und TAN in einem Formular innerhalb einer E-Mail anzugeben. Auch telefonisch wird Ihre Bank Sie nie nach sensiblen Daten fragen. Wenn Sie sich unsicher sind, rufen Sie direkt unter der Ihnen bekannten Nummer Ihre Bank an und rückversichern Sie sich.
- Phishing-E-Mails sind in manchen Fällen in schlechtem Deutsch verfasst. Umlaute wie ä, ö, ü fehlen mitunter. Das liegt daran, dass diese Nachrichten von Computerprogrammen aus anderen Sprachen schnell und einfach übersetzt werden.
- Am sichersten ist es, nie über einen E-Mail-Link auf eine Webseite zu gehen. Rufen Sie die Seite immer direkt aus Ihrem Browser heraus auf. Achten Sie darauf, dass die Adresse der Seite korrekt geschrieben ist.

Aufpassen bei Phishing-Webseiten.

- Achten Sie immer auf das Sicherheitszertifikat, das durch das Sicherheitsschloss-Symbol in der unteren rechten Ecke Ihres Browsers angezeigt wird. Ist dieses nicht vorhanden, handelt es sich um eine nicht sichere Seite.
- Wenn es sich um eine sichere Verbindung handelt, wird das Kürzel „https://" in der Adresszeile des Browsers angezeigt. Dieses Verschlüsselungsverfahren verhindert, dass die Daten in der Zeit, in der Sie daran arbeiten, gelesen oder manipuliert werden können. In den seltensten Fällen kann auch das gefälscht sein. Um sicherzugehen, geben Sie die Adresse Ihrer Bank immer selbstständig in die Adresszeile Ihres Browsers ein und folgen keinem Link.
- Auf der Login-Seite werden von Ihrer Bank nie TAN-Codes abgefragt. Sollte das der Fall sein, setzen Sie sich bitte unverzüglich mit Ihrer Bank in Verbindung.

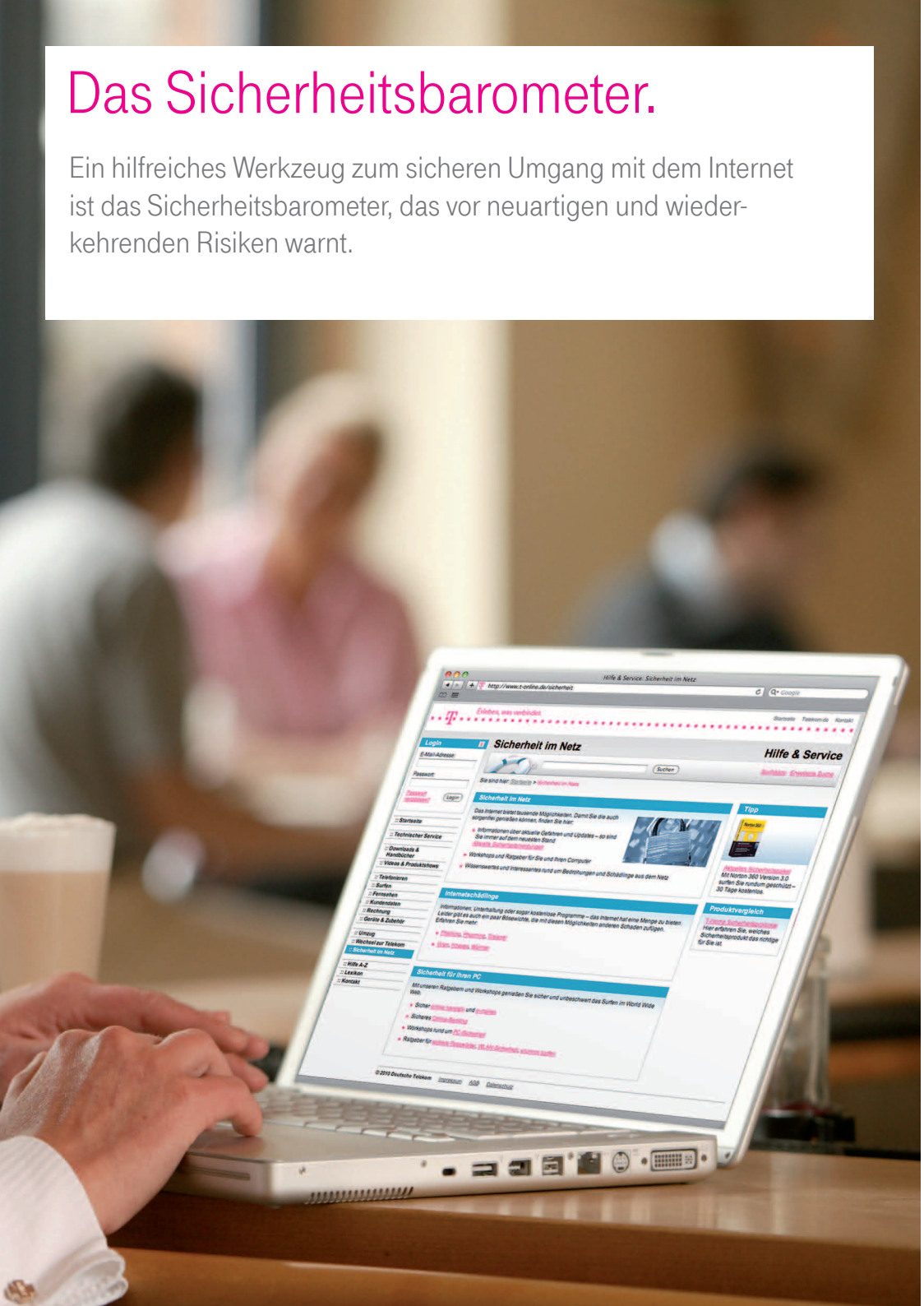
Generelle Vorsichtsmaßnahmen beim Online-Banking.

- Bewahren Sie Ihre persönlichen Daten wie Passwörter, PIN und TAN immer an einem sicheren Ort auf und speichern Sie diese nie auf Ihrem PC ab, auch nicht in einem sogenannten Passwort-Manager. Sind diese Daten auf dem PC gespeichert, könnten sie ausgelesen werden.
- Gestalten und verwahren Sie Ihr Passwort sicher (siehe „Gestaltung eines sicheren Passwortes"). Für das Online-Banking sollten Sie auf jeden Fall ein spezielles Passwort verwenden, das Sie nicht für andere Zwecke nutzen. Das Kennwort sollte regelmäßig geändert werden, um die Sicherheit zu erhöhen.
- Bankgeschäfte sollten nur vom eigenen privaten PC oder Mobilfunkgerät im privaten Umfeld durchgeführt werden. Achten Sie darauf, sich nach Beendigung der Sitzung abzumelden und den Zwischenspeicher (→ **Cache**) Ihres PCs zu leeren.
- Wichtig ist auch hier, dass Sie immer eine aktuelle Virenschutzsoftware benutzen und Sicherheits-Updates durchführen, um Sicherheitslücken zu schließen.
- Überprüfen Sie regelmäßig Ihre Kontobewegungen. Setzen Sie sich unverzüglich mit Ihrer Bank in Verbindung, wenn Ihnen etwas verdächtig vorkommt oder Unstimmigkeiten auftreten. Das rät auch der Bundesverband Deutscher Banken.

Wenn Ihnen etwas verdächtig oder ungewöhnlich erscheint, sperren Sie Ihren Zugang zum Online-Banking. Dies können Sie telefonisch bei Ihrer Bank in Auftrag geben oder direkt über eine entsprechende Funktion im Online-Banking-Fenster veranlassen.

Das Sicherheitsbarometer.

Ein hilfreiches Werkzeug zum sicheren Umgang mit dem Internet ist das Sicherheitsbarometer, das vor neuartigen und wiederkehrenden Risiken warnt.



Das Sicherheitsbarometer sowie aktuelle Informationen rund um das Thema „Online-Sicherheit“ finden Sie auch unter **www.t-online.de/sicherheit** auf den Serviceseiten der Deutschen Telekom.

Die aktuelle Gefahrenlage zeigt das Barometer in vier Stufen an:

- **Die Stufe Grün wird als „Normales Risiko“** bezeichnet und informiert, wie sich Nutzer schützen sollten, damit der Grundschutz möglichst hoch ist.

- **Die Stufe Gelb wird als „Erhöhtes Risiko“** bezeichnet und hat die Aufgabe, die Nutzer vor akuten Bedrohungen zu warnen, deren Verbreitung oder Schadensausmaß allerdings begrenzt sind. Beispiele sind → **Phishing**- oder → **Pharming**-Angriffe mit begrenztem Ausmaß.

- **Die Stufe Orange wird als „Hohes Risiko“** bezeichnet und soll die Nutzer vor akuten Bedrohungen warnen, deren Verbreitung oder Schadensausmaß signifikant sind.

- **Die Stufe Rot wird als „Internet-Alarm“** bezeichnet und soll die Nutzer vor aktuellen Bedrohungen warnen, die die Verfügbarkeit oder Integrität von PCs und Netzwerken in großem Ausmaß gefährden.

In Zeiten normaler Risikolage, das heißt, wenn keine akuten Warnungen vorliegen, informiert das Barometer über die Basis-Sicherheitsmaßnahmen und sensibilisiert für aktuelle sicherheitsrelevante Themen oder Bedrohungen. Die Zielgruppe des Barometers sind Privatanwender und kleine Unternehmen, die eine gängige Anbindung an das Internet über DSL, ISDN oder Modem nutzen.

Verhalten im Sozialen Netzwerk.

Durch das Web 2.0 haben die Sozialen Netzwerke Einzug in unseren Alltag gehalten.

Jeder ist heutzutage in der Lage, Informationen in die Welt zu senden und zu empfangen, und so geben Mitglieder von Sozialen Netzwerken wie Xing, Facebook, MySpace, StudiVZ etc. wie selbstverständlich private Daten preis. Das Internet ist kein rechtsfreier Raum. Dennoch halten sich nicht alle an die geltenden Datenschutzbestimmungen, an die Regelung zum Recht am eigenen Bild oder an die Urheberrechte. Dies schafft Risiken für die Privatsphäre, derer sich viele Nutzer nicht bewusst sind. **Aus diesem Grund ist es wichtig, sich an bestimmte Umgangsformen in Sozialen Netzwerken zu halten.**

Vorab: Lesen Sie die Allgemeinen Geschäftsbedingungen und Datenschutzhinweise der Plattform-Betreiber genau. Aus ihnen ergibt sich in aller Regel, wie die Betreiber mit Ihren persönlichen Daten umgehen.

Gestaltung des eigenen Profils.

- In erster Linie gilt es, möglichst keine persönlichen Daten wie E-Mail-Adressen, Telefonnummern, Messenger-Daten, Fotos etc. preiszugeben. Denn wer viel über sich verrät, macht es anderen leicht, ihm beispielsweise Phishing-Nachrichten oder unerwünschte Werbung zukommen zu lassen.

- In Chats und Diskussionsforen können Sie anstelle des eigenen Namens auch einen Spitznamen angeben, auch wenn die Betreiber dieser Sites dazu aufrufen, den richtigen Namen zu nennen. Wenn Sie dennoch nicht auf Ihren eigenen Namen verzichten möchten, sollten Sie zumindest den Nachnamen zum Initial abkürzen.

- Den Zugriff auf das eigene Profil können Sie bei den Einstellungen einschränken. Am sichersten ist es, nur Freunden den Zugang zu erlauben.

Profilbilder.

- Auch wenn es bei den jungen Netzwerknutzern normal scheint, sich anhand von Fotos im Internet darzustellen, missachten zu freizügige Bilder die Regeln zum Schutz der Privatsphäre. Aus diesem Grund sollten Sie sich gut überlegen, welche Fotos Sie von sich im Internet zeigen. Fotos in Strandkleidung oder Unterwäsche sind grundsätzlich tabu. Die meisten Menschen würden im Alltag kaum Unbekannten ihr Privatleben offenbaren, oder? Bedenken Sie also stets, was Sie wirklich von sich preisgeben wollen.

Fotoalben.

- Die Funktion, Fotos in Online-Fotoalben hochzuladen, wird oft und gerne genutzt. Um auch hierbei kein Risiko einzugehen, sollte man darauf achten, nur direkten Freunden Zugang zu diesen Alben zu gewähren.

- Grundsätzlich sollte man nur die Fotos hochladen, an denen man auch die Rechte besitzt.

- Fotos, die Sie einmal ins Internet hochgeladen haben, bleiben oft lange im **→ Cache** gespeichert, auch wenn Sie die Bilder oder auch das ganze Fotoalbum wieder löschen.

Privatsphäre.

- Alle Einstellungen, die ein Soziales Netzwerk zum Schutz der Privatsphäre anbietet, sollten Sie kennen und gegebenenfalls auch nutzen.

Wie Sie in den verschiedenen Sozialen Netzwerken Ihre Privatsphäre richtig schützen, können Sie im Internet auf der Seite **www.klicksafe.de** nachlesen.

Freunde hinzufügen.

- Oft erhalten Sie eine Freundschaftseinladung von jemandem, den Sie nicht kennen. Bevor Sie eine Einladung annehmen oder an andere verschicken, sollten Sie gründlich prüfen, um wen es sich dabei handelt.

- Persönliche Daten sollten nur echten Freunden zugänglich gemacht werden.

- Da Sie selbst nicht auf unvorteilhaften Bildern gezeigt werden oder private Kommentare über sich auf den Pinnwänden dieser Sites lesen möchten, sollten Sie auch die Privatsphäre von Freunden und Bekannten respektieren und erst nach Absprache Bilder von ihnen ins Netz stellen.

Da jeder „Freund“ die für Freunde freigegebenen Daten sehen kann, sollten Sie sich immer gut überlegen, wen Sie als solchen aufnehmen.

Verabredungen im Internet.

- Soziale Netzwerke werden häufig dafür genutzt, sich mit Freunden zu verabreden oder andere Termine zu besprechen. Private Informationen wie Verabredungen oder „Ich bin heute Abend allein zu Hause“ sollten jedoch auf keinen Fall auf den Pinnwänden angegeben werden. Solche Informationen sollte man nur privat, zum Beispiel per E-Mail oder Messenger wie von ICQ, Skype etc., austauschen!

Melde- und Ignorierfunktion.

- Personen, Inhalte oder Gruppen, die gegen den Verhaltenskodex der Netzwerke verstoßen, sollten Sie unbedingt melden. Sie können entweder den Melde-Button auf Ihrer Profilseite dafür nutzen oder sich an Ihre örtliche Polizeidienststelle wenden.

- Nutzern, die Sie belästigen, können Sie mit Hilfe der Ignorierfunktion den Zugang zu Ihrer Seite versperren. Diese können Ihnen dann auch keine Nachrichten mehr schicken. Zusätzlich sollten Sie diese Personen auch bei Ihrem Anbieter melden.

Sicherheit für Kinder im Internet.

In der heutigen Zeit ist der Umgang mit dem Internet bereits im Kindesalter fast selbstverständlich. Kein Wunder, dass sich Eltern um die Sicherheit ihrer Kinder sorgen, wenn diese das Internet nutzen.

Es gibt jedoch Möglichkeiten, dieser Sorge vorzubeugen. So sensibilisieren Sie Ihr Kind für den richtigen Umgang mit dem Internet:

- Entdecken Sie das Internet gemeinsam, damit Ihr Kind von Anfang an den richtigen Umgang damit lernt! Sie sollten außerdem regelmäßig nach neuen Erfahrungen im Internet fragen und/oder einen Blick auf den Bildschirm werfen, wenn Ihr Kind am PC sitzt.

Auf der Internetseite **www.klick-tipps.net** können Sie sich zusammen mit Ihrem Kind informieren, auf welchen Seiten Kinder surfen können, ohne befürchten zu müssen, mit ungeeigneten Inhalten konfrontiert zu werden. In der Initiative **www.ein-netz-fuer-kinder.de** fördert die Deutsche Telekom kindgerechte Angebote im Internet und schafft einen sicheren Surfraum – etwa mit der Suchmaschine **www.fragfinn.de**.

- Vereinbaren Sie Regeln für die Internetnutzung und informieren Sie sich in diesem Zusammenhang über Schutzvorrichtungen. Es gibt spezielle Filter, die auf dem Computer installiert werden und pornografische, gewaltverherrlichende oder rechtsradikale Seiten automatisch sperren. **www.millionen-fangen-an.de/#/Kinderschutzsoftware**

- Persönliche Daten sollte Ihr Kind keinesfalls weitergeben – keine Angaben zum Alter, zum Wohnort oder zu Treffpunkten. Sogar bei der Erstellung einer E-Mail-Adresse oder eines Namens für Chaträume sollte Ihr Kind ausschließlich auf Spitznamen zurückgreifen.

- Sprechen Sie über Risiken von Treffen! Im Internet kennengelernte Personen sollte Ihr Kind nur nach Rücksprache mit Ihnen treffen. Kinder können nicht erkennen, ob diese Person gut gemeinte Absichten hat.

- Diskutieren Sie den Wahrheitsgehalt von Inhalten mit Ihren Kindern!

- Ermutigen Sie Ihr Kind zu guter Netiquette, also zu angemessenem Verhalten! Dies ist besonders dann wichtig, wenn Ihr Kind im Internet mit Fremden in Kontakt tritt.

- Nutzen Sie Filterprogramme, damit Ihr Kind nur einen eingeschränkten Zugang zum Internet hat und nur altersgerechte Seiten besucht!

- Weitere umfassende Informationen zum Thema Sicherheit im Netz finden Sie auf der Seite **www.klicksafe.de**, die im Auftrag der Europäischen Kommission die Medienkompetenz im Umgang mit dem Internet fördern soll.

Wie schützt man sich vor unerlaubten Werbeanrufen?

Werbeanrufe ohne die Einwilligung der Verbraucher waren schon vor der Gesetzesänderung im August 2009 verboten.

Solche unerwünschten Werbeanrufe stellen nach dem Gesetz gegen den unlauteren Wettbewerb eine unzumutbare Belästigung dar. Seit der Änderung werden Verstöße gegen dieses Gesetz mit hohen Bußgeldern (bis zu 50.000 Euro) bestraft.

Unter welchen Bedingungen dürfen Sie zu Werbezwecken angerufen werden?

- Damit Sie zu Werbezwecken angerufen werden dürfen, müssen Sie eine Einwilligung erteilen. Hierzu müssen Sie darüber informiert sein, welche Daten von wem für welchen Zweck verwendet werden sollen. Der Text, mit dem Sie Ihre Einwilligung abgeben, muss Ihnen beispielsweise deutlich machen, wer Sie für Werbezwecke anrufen möchte.

- Ihre Einwilligung muss freiwillig sein, das heißt auf Ihrer freien Entscheidung beruhen. Wenn Sie vermuten, dass Ihnen die Einwilligung untergeschoben wird, oder Sie das Gefühl haben, zur Abgabe der Einwilligung gezwungen zu werden, sollten Sie Ihre Zustimmung verweigern.

- Für die Deutsche Telekom ist das Vorliegen einer Einwilligung des Verbrauchers in die telefonische Werbung Voraussetzung für einen Werbeanruf.

- Werbeanrufe ohne Anzeige der Rufnummer sind laut neuem Gesetz nicht mehr erlaubt.

- Wenn Sie von Unternehmen angerufen werden, deren Kunde Sie niemals waren, können Sie von Ihrem Auskunftsrecht Gebrauch machen. Das Bundesdatenschutzgesetz (BDSG) beinhaltet weitgehende Auskunftsrechte für die Verbraucher.

Nach § 34 Bundesdatenschutzgesetz (BDSG) können Sie über die folgenden Sachverhalte im Unternehmen Auskunft verlangen:

- die zu Ihrer Person gespeicherten Daten, dazu gehört auch die Herkunft dieser Daten

- Empfänger, an die diese Daten weitergegeben werden/wurden

- den Zweck der Speicherung

Beschweren Sie sich in jedem Fall bei dem Unternehmen, das die Werbeanrufe veranlasst hat, und untersagen Sie ihm gegebenenfalls die weitere Nutzung Ihrer Daten für Werbezwecke.

Wie Sie vorgehen können, wenn Sie trotz allem ohne Zustimmung angerufen werden:

Zur Aufdeckung dieser unerwünschten Werbeanrufe bittet die Bundesnetzagentur um die Mithilfe der Verbraucher. Im Falle von Werbeanrufen, die Sie ohne Ihr Einverständnis erhalten, sollten Sie sich unbedingt die folgenden Daten notieren:

- Datum und Uhrzeit des Anrufs
- den Namen des Anrufers und des Unternehmens, für das er tätig ist
- falls möglich die Telefonnummer (die Unterdrückung der Rufnummer bei Werbeanrufen stellt einen Verstoß gegen das Telekommunikationsgesetz dar und wird mit bis zu 10.000 Euro Bußgeld bestraft)
- den Grund des Anrufs

Diese Informationen können Sie auf der Internetseite der Bundesnetzagentur eingeben (**www.bundesnetzagentur.de**). Die Regulierungsbehörde kann dann nach eigener Prüfung ein Ordnungswidrigkeitenverfahren einleiten.

Kurzes Datenschutz-Glossar.

→ **Anti-Spyware** bezeichnet Programme, die das Ausspionieren von Userdaten durch → **Spyware**-Programme verhindern.

→ **Bluetooth** stellt eine Vernetzung von zwei Endgeräten über Funk über eine kleine Distanz her, wodurch Daten ausgetauscht werden können.

→ **Cache** wird umgangssprachlich auch als Zwischenspeicher bezeichnet. Dabei werden Inhalte vom PC selbstständig gespeichert, damit sie beim wiederholten Aufruf schneller zur Verfügung stehen.

→ **Firewall** überwacht den Datenfluss in einem Netzwerk und sichert die Verbindung nach außen vor unerlaubtem Zugriff ab. Dabei prüft die Firewall nach vorher definierten Regeln, ob Datenpakete, zum Beispiel zwischen PC und Internet, verschickt werden dürfen.

→ **HotSpots** sind öffentlich zugängliche WLAN-Zugänge. Sie bieten die Möglichkeit, sich per Notebook, PDA oder Handy mit dem Internet zu verbinden. Die öffentlichen Internetzugänge befinden sich häufig an öffentlichen Plätzen wie Bahnhöfen, Hotels, Cafés und Flughäfen und werden in den meisten Fällen gegen Bezahlung bereitgestellt.

→ **MAC-Adresse** (Media-Access-Control-Adresse, auch Ethernet-ID oder Airport-ID bei Apple oder Physikalische Adresse bei Microsoft genannt) ist die Hardwareadresse jedes einzelnen Netzwerkadapters. Sie dient zur eindeutigen Identifizierung des Geräts in einem Rechnernetz.

→ **Pharming** bezeichnet eine spezielle Betrugsmethode im Internet. Dabei werden bestimmte Webbrowser manipuliert, um die User auf eine gefälschte Website umzuleiten. Häufig wird diese Methode bei Internetseiten von Banken angewendet. Pharming ist eine Weiterentwicklung von Phishing.

→ **Phishing** werden die Versuche genannt, über gefälschte Internetadressen an Daten eines Internetbenutzers zu gelangen. Der Begriff setzt sich zusammen aus den englischen Begriffen „Password“ und „Fishing“, also „Passwort-Angeln“.

→ **PIN** Dieses Kürzel steht für „Persönliche Identifikationsnummer“. Es handelt sich hierbei um eine Geheimzahl oder einen Code aus Zahlen und Buchstaben, den Sie benötigen, um sich beispielsweise beim Online-Banking Zugang zu Ihrem Konto verschaffen zu können.

→ **Spyware**-Programme bezeichnet man auch als Schnüffelprogramme, die Informationen und Daten des Users ohne dessen Wissen an den Hersteller senden. Um das Spionieren zu verhindern, installiert man → **Anti-Spyware**-Programme.

→ **SSID** Kurz für Service Set Identifier oder auch Network Name. Dies ist die Kennung eines Funknetzwerks.

→ **TAN** Kurz für Transaktionsnummer. Dies ist ein Einmalpasswort, das hauptsächlich beim Online-Banking benötigt wird und meist aus sechs Dezimalziffern besteht.

→ **Trojaner** Ein Trojanisches Pferd, kurz Trojaner, ist ein Computerprogramm, das vorgibt, eine nützliche Anwendung zu sein. Im Hintergrund führt es jedoch andere, meist schädliche Anwendungen aus, von denen der Benutzer nichts weiß.

→ **Viren** sind Computerprogramme, die sich selbstständig verbreiten. Auf diesem Wege schleusen sie sich in andere Computerprogramme ein und vervielfältigen sich dort. Einmal gestartet, kann ein solches Programm vom Anwender nicht mehr kontrolliert werden und nimmt Einfluss beispielsweise auf den Status der Hardware, das Betriebssystem oder die Software. Die Bezeichnung „Viren“ bezieht sich hierbei auf die infektionsartige Verbreitung.

→ **Web 2.0** ist eine Weiterentwicklung des World Wide Web. Durch die Weiterentwicklung hat sich die Nutzung des Internets verändert. Der Blog, Wikipedia und Flickr sind nur einige Beispiele, die durch das Web 2.0 möglich geworden sind.

→ **WLAN** Abgeleitet vom englischen Begriff „Wireless Local Area Network“ und bedeutet wörtlich „drahtloses lokales Netzwerk“.

→ **WPA2-PSK** Dies bezeichnet eine Verschlüsselungsmethode für Drahtlosnetzwerke.

→ **Würmer** sind schädliche Programme, die sich über Computernetzwerke verbreiten. Um sich verbreiten zu können, benötigt der Wurm Netzwerkdienste oder Benutzerinteraktionen. Die Übertragungskanäle von Computerwürmern sind zum Beispiel E-Mails oder Software-Downloads aus dem Internet.

Machen Sie sich immer bewusst, wie sensibel Daten sind, und versehen Sie Ihren PC mit möglichst hohen Sicherheitseinstellungen.

Versehen Sie Ihre Daten, E-Mail-Konten und Internetzugänge wenn möglich mit einem Passwort. Wichtig ist dabei, eine Kombination aus Buchstaben und Zahlen zu wählen, die niemand außer Ihnen kennt.

Nutzen Sie kein freies WLAN, dessen Betreiber Sie nicht kennen, und sichern Sie Ihren Zugang zu Hause stets mit einem Passwort.

Bewahren Sie Ihre Zugangsdaten (Passwörter und Benutzernamen) niemals an einem leicht zugänglichen Ort auf und speichern Sie diese nicht auf Ihrem PC.

Geben Sie so wenig wie möglich über sich im Internet preis. Angaben wie E-Mail-Adressen und Telefonnummern oder das Hochladen von Fotos sollten Sie sich gut überlegen.

Achten Sie darauf, welche Seiten Ihre Kinder im Internet besuchen, und klären Sie sie über mögliche Gefahren auf.

Zeigen Sie unerlaubt getätigte Werbeanrufe bei der Bundesnetzagentur an.

Machen Sie in regelmäßigen Abständen Sicherheitskopien von Ihren Daten.

Halten Sie Ihre Virenschutzsoftware immer auf dem neuesten Stand.

Achten Sie darauf, dass Sie an einem öffentlich zugänglichen PC niemandem Einsicht in Ihre Daten ermöglichen.

Worauf Sie unbedingt achten sollten!

Herausgeber
Deutsche Telekom AG
Corporate Communications / Group Privacy
Friedrich-Ebert-Allee 140
53113 Bonn
www.telekom.com/datenschutz

Kontakt
datenschutz@telekom.de

KNr. 642 100 045 | Stand 06/2010

Erleben, was verbindet.